Blaine J. Benard (#5661)
Brent E. Johnson (#7558)
Engels J. Tejeda (#11427)
Emily T. Howe (#18294)
HOLLAND & HART LLP
222 South Main Street, Suite 2200
Salt Lake City, UT 84101-2194
Telephone: 801.799.5800
BJBenard@hollandhart.com
BJohnson@hollandhart.com
EJTejeda@hollandhart.com
ETHowe@hollandhart.com

Attorneys for Defendant Uintah Basin Healthcare

**IN THE UNITED STATES DISTRICT COURT,
FOR THE DISTRICT OF UTAH, CENTRAL DIVISION**

JASON RASMUSSEN et al., on behalf of themselves and all others similarly situated, Plaintiffs, vs. UINTAH BASIN HEALTHCARE, a Utah non-profit corporation, Defendant.	**DECLARATION OF DR. BRUCE V. HARTLEY IN SUPPORT OF DEFENDANT'S REPLY IN SUPPORT OF ITS MOTION TO DISMISS PLAINTIFFS' COMPLAINT UNDER FEDERAL RULES OF CIVIL PROCEDURE 12(B)(1) AND 12(B)(6), OR IN THE ALTERNATIVE, SUMMARY JUDGMENT UNDER RULE 56** 2:23-cv-00322-HCN-DBP Judge Howard C. Nielson, Jr. Chief Magistrate Judge Dustin B. Pead

I, Dr. Bruce V. Hartley, CISSP, declare as follows:

1. I have personal knowledge of the facts in this declaration and, if called to testify as a witness, I would testify under oath as to these facts.

2. The opinions made herein are based upon my personal knowledge, professional experience and upon my review of relevant records, documents, and information.

3. A copy of my CV detailing my most relevant experience is attached to my October 16, 2023 Declaration as **Ex. 16**.

4. My relevant experience is described in more detail in my October 16, 2023 Declaration. I reiterate here that I am currently the Managing Director of Arete Advisors, Inc., where I lead the Advisory practice. Arete Advisors is a Cyber Security firm that focuses on data-centric investigations, incident response, and security assessments. The Advisory practice provides digital investigations and expert services, including the delivery of high-quality cyber security, incident response, digital investigations, and expert witness services across the company. I am currently leading several digital investigations and data security incident responses as well as providing expert witness services related to cyber security and/or trade secret issues involving several firms in the information technology space.

5. In addition to my current position as Managing Director of Arete Advisors, I have held other senior executive and technical management positions in numerous organizations as a Chief Information Officer, Chief Technology Officer, Chief Information Security Officer, and a National Service Line Leader at a "Big 4" professional services firm. Prior to Arete, I was the Chief Technology Officer and Chief Information Security Officer at Discovia. Prior to Discovia, I was Vice President of the Celerity Consulting Group, where I led the Digital Forensics and Investigations practice. Prior to Celerity, I was the National Director for Discovery Services at Deloitte FAS, LLP. Before joining Deloitte, I was the Chief Technology Officer at Cricket Technologies and the IT Sector Director (CIO) at bd Systems, Inc. (now part of SAIC).

6. I am recognized by the National Computer Security Center as a Vendor Security Analyst (VSA) and certified by the ISC² as a Certified Information System Security Professional (CISSP).

7. I have extensive experience across the entire information technology, software engineering, and cyber security and digital forensic spectrum, which is described in more detail in my October 16, 2023 Declaration.

8. Arete's cyber threat intelligence team understands the geography of the dark web as well as how cybercriminals behave in terms of what they exploit and how they monetize what they've stolen. Arete has the resources to find stolen or disclosed data and contextualize risks. Through dark web monitoring, Arete can search for threat actors who may be auctioning off or displaying a company's or individual's information, monitor for access credentials, business data, and hidden threats, such as insider fraud, software/hardware vulnerabilities, and zero-day threats.

9. Uintah Basin Healthcare ("UBH") informed me that on November 7, 2022, threat actors attacked UBH's computer network (the "Incident").

10. Under my direction, my team conducted a comprehensive retroactive search for Plaintiffs' data across 1,500+ dark and surface web sources. This included but is not limited to attempts to auction, advertise, or otherwise post datasets associated with UBH; monitor actor forums, chat channels, and marketplaces for conversations surrounding UBH (Telegram, Breached forum, RAMP, RAID forum, etc.), infrastructure threats such as infected hosts, monitor open-source repositories, credentials associated with UBH's accounts on dark web credential shops, past or current malware attempting to communicate with UBH's externally

facing infrastructure, potential phishing attacks, search for Advertisements, discussions, or mentions of datasets associated with UBH in open-source repositories such as Github.

11. We conducted the comprehensive retroactive search by running searches with the following search terms, Plaintiffs' full name AND "Utah," OR plaintiffs' date of birth, OR address, OR phone number, OR email, OR a portion of their social security number. For Plaintiff A[redacted] K[redacted] we ran the following searches: full name AND "Utah," OR date of birth, OR address, OR phone number.

12. Our dark web search resulted in no hits of Plaintiffs' personal information related to the UBH Incident although our searches did discover that Plaintiffs' personal information was already on the dark web which were linked to previous data breaches not associated with UBH.

13. Specifically, our search concluded that:

a. Plaintiff Jason Rasmussen's personal information was not disclosed on the dark web from the UBH Incident.

b. Plaintiff Mindy Rasmussen's personal information was not disclosed on the dark web from the UBH Incident.

c. Plaintiff Donna Halton's personal information was not disclosed on the dark web from the UBH Incident.

d. Plaintiff Doris Hyatt's personal information was not disclosed on the dark web from the UBH Incident.

e. Plaintiff A[redacted] K[redacted] personal information was not disclosed on the dark web from the UBH Incident.

f. Plaintiff Christian Miller's personal information was not disclosed on the

dark web from the UBH Incident.

14. The search did identify that several of the Plaintiffs do have personal information on the dark web, but all exposures are from separate, third-party data breaches, not the UBH Incident.

15. A third-party breach occurs when an individual uses their personal or company email address to register for a website, and that website subsequently suffers a data breach.

16. Jason Rasmussen's UBH email address was exposed by a third-party breach. The third-party breach was an April 2021 LinkedIn database breach.

17. Christian Miller and Jason Rasmussen's names appear in data dumps from third-party breaches previously on sale on known threat actor marketplaces.

18. Christian Millers' name appears in data dumps from third-party breaches of fashionava, Instacart, and wiggle.co.uk.

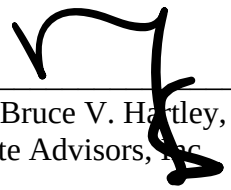
19. Jason Rasmussen's name appears in data dumps from third-party breaches of Postmates.

20. In my professional opinion, the UBH Incident did not result in any of Plaintiffs' personal information being exposed on the dark web.

[remainder of page intentionally left blank]

I declare under penalty of perjury under the laws of the State of Utah and the United States that the foregoing is true and correct.

Executed this 16th day of January, 2024.



Dr. Bruce V. Hartley, Managing Director
Arete Advisors, Inc.